March 15, 2019

Electronically submitted to submissions@banking.senate.gov

Senator Mike Crapo, Chairman
Senator Sherrod Brown, Ranking Member
Senate Committee on Banking, Housing,
and Urban Affairs Committee
United States Senate
Washington, DC 20510

Re: Feedback on Data Privacy, Protection and Collection

Dear Chairman Crapo and Ranking Member Brown:

The undersigned consumer, community, privacy, legal services and advocacy groups are pleased to submit this response to your Call for Feedback on Data Privacy, Protection, and Collection. This response will primarily focus on credit and consumer reporting issues, including ideas to amend the Fair Credit Reporting Act (FCRA) and improve consumer rights with respect to consumer reporting agencies (CRAs), including the Big Three nationwide CRAs (Equifax, Experian, and TransUnion).

Question 1: *What could be done through legislation, regulation, or by implementing best practices that would give consumers more control over and enhance the protection of consumer financial data, and ensure that consumers are notified of breaches in a timely and consistent manner?*

a. **Make credit reports frozen by default.** With respect to credit and consumer reporting, one way to give consumers control over their data is to make consumer reports frozen by default. Freezing reports by default will not only give consumers much more control over their own data, it will also be a strong preventative measure to deter identity theft. The switch for access to consumer reports under the FCRA should automatically be set to "off." Consumers, not CRAs, should have the right to decide when to turn the switch "on." And in the process of turning the switch on, CRAs should be required to verify the identity of the consumer to make sure it is really them. In the 115th Congress, we supported S.2362, the Control Your Personal Credit Information Act of 2018, introduced by Senator Reed. We would be supportive of a similar bill if reintroduced.

b. **Security freezes should be part of a "one-stop shopping" website**. If Congress does not make consumer reports frozen by default, *i.e.* if security freezes remain opt in, Congress should make it much easier for consumers to obtain freezes. For example, Congress should require the nationwide CRAs (*i.e.*, Equifax, Experian, TransUnion) to set up a "one-stop shopping" website to engage in transactions with them. Consumers should be able to obtain free access to their credit reports online (see answer to Question 2), challenge errors, and freeze their reports all in one place. The security freezes should be just as easy to access as the unregulated "locks" that the nationwide CRAs now provide, in some cases only with their paid services.

c. **States have led the way in protecting consumers when data breaches occur and should not be prevented from continuing to do so**. In terms of data breach notifications, all 50 states already have laws that govern this issue. If Congress acts, the most important element of any breach notification law is that it should not preempt any state law that is stronger and provides more protections. States have always led the way in robust and pioneering measures for consumer protection and privacy, and should not be blocked from further innovation. Furthermore, any Congressional bill should follow the strongest elements of the state data breach laws such as requiring notification whenever information may be compromised, regardless of whether there is a likelihood of harm, and covering a broad scope of consumer data. Other important elements of any federal privacy law, such as allowing for state and private enforcement, are set forth in the Public Interest Privacy Legislation Principles, attached to this response.

Question 2: *What could be done through legislation, regulation, or by implementing best practices to ensure that financial regulators and private financial companies (including third-parties that share information with financial regulators and private financial companies) provide adequate disclosure to citizens and consumers about the information that is being collected about them and for what purposes?*

a. **Nationwide CRAs should be required to provide unlimited online access to file disclosures as part of a one-stop shopping portal.** With respect to credit reporting, it is time to require the nationwide CRAs, *i.e.*, Equifax, Experian, and TransUnion, to improve disclosures by providing unlimited online access to our credit files. The nationwide CRAs already provide this type of access, albeit in the form of a paid product, so they have already developed the software and systems to make this easily available. Why do we allow the nationwide CRAs to make $20 per month selling us back our own information? *See, e.g.*, https://www.transunion.com/credit-monitoring ("TransUnion's credit report monitoring service gives you frequent access to your credit history, so you can check your credit report as often as you like."), viewed March 2, 2019. The nationwide CRAs, and indeed all CRAs, earn big bucks selling our data to creditors, debt collectors, employers, and others. The least they can do to compensate us is to provide us free access to our own data at any time.

In general, the nationwide CRAs should be required to develop "one-stop shopping" online consumer portals, with accompanying mobile applications, that give consumers free access to:

- Unlimited disclosure of their credit reports;
- Unlimited or monthly disclosure of their credit score;
- The ability to opt-out of having their consumer reports used for prescreening and for all other uses for non-consumer report information held by the nationwide CRAs;
- The ability to initiate a dispute;
- The ability to place, thaw or remove security freezes; and
- Information on who has accessed their credit report and for what purpose.

A one-stop shopping portal was proposed by Senators Kennedy and Schatz in 2018, as part of a draft Fair and Accurate Information Reporting (FAIR) for Consumers Act. We would support such a bill if introduced.

b. **There should be a free right to a credit score and required disclosure of any other risk scores.** Another improvement to disclosures that is long overdue would be the right to a free credit score under the FCRA. While there have been many voluntary improvements for access to free credit scores, such as FICO's Open Access Initiative, consumers should have a legal right to a free credit score. Furthermore, this required disclosure should be for a credit score that is widely used by lenders, and not the "educational" scores offered by the nationwide CRAs that no lenders actually use.

In additional, consumers should have the right to access any other "risk score" based on a consumer report, such as scores issued by tenant screening CRAs, background check CRAs, and CRAs focused on healthcare payment information (e.g. PARO scores). A fundamental principle for data privacy and protection is that if a company holds and sells or shares information about consumers, we should be entitled to access that information.

c. **There should be a registry for all CRAs.** The FCRA currently does not require a CRA to register or self-identify to any regulator as such. As discussed in our answer to Question 5, the definition of "consumer reporting agency" is very broad. There are likely hundreds of CRAs, ranging from very small (possibly one person) businesses to the huge sprawling multinational corporations. Each of these CRAs assembles or evaluates information about consumers, about us. In addition, a growing number of companies gather and disseminate consumer data for purposes covered by the FCRA without considering themselves CRAs. But because there is not a complete list of these CRAs, consumers do not have full information on which companies or entities hold or use their personal information, and regulators do not know what companies are or are not complying with their FCRA duties. To address this gap, there should be a registry, either at the CFPB or FTC, of all consumer reporting agencies that fall under the FCRA. Consumers could check this registry to see which companies may be using their information. In order to publish such a register, all CRAs must be required to register with the CFPB/FTC. We note that, once again, states are in the forefront of this issue, as the state of Vermont has recently enacted a requirement for a registry of data brokers. Vt. Stat. Ann. Tit. 9, § 2446. We would also support a registry for all data brokers, or better yet as discussed in the response to Question 5, to bring data brokers under the regulation of the FCRA.

d. **Consumers should receive a copy of the consumer report that factored into an adverse action.** One measure to improve disclosures to consumers under the FCRA is to require users to provide a copy of the actual consumer report when it is used adversely against a consumer. Currently, the FCRA only requires the user of a consumer report to provide a notice to consumers if they take an adverse action against them based on the report. 15 U.S.C. § 1681m. The notice informs the consumer that a consumer report was used against them, and must include a credit score if one was used, but does not actually provide a copy of the report. The consumer must independently request a report from the CRA, and that report may be very different from the consumer report used to take the adverse action.

The exception to this rule is if the report was used for employment purposes, in which case the employer must provide a copy of the actual report used in the adverse employment decision. 15 U.S.C. § 1681b(b). This latter requirement should be extended to all uses of a consumer report,

i.e., the FCRA should require all users of consumer reports to provide a copy of the same report to consumers if the report is used to take an adverse action against them.

Question 3: *What could be done through legislation, regulation, or by implementing best practices to give citizens and consumers control over how financial regulators and private financial companies (including third-parties that share information with financial regulators and private financial companies) use consumer data?*

a. **Freeze credit and consumer reports by default**. With respect to FCRA-covered companies, the strongest and simplest way to give consumers complete control over their own data is to freeze consumer reports by default, discussed in our answer to Question 1. This would prevent credit reports and other consumer reports from being shared unless consumers have opted in.

b. **Consumers should have control over non-FCRA covered uses of their personal data.** In addition to freezing credit reports by default, all commercial and most governmental use of other consumer data should be opt-in only. There should be a regime similar to the one in effect in the European Union, *i.e.*, the General Data Protection Regulation (GDPR), requiring consent to use of our personal data.

Other important elements of any privacy laws are set forth in the Public Interest Privacy Legislation Principles, attached to this response, and include:

1. Privacy protections must be strong, meaningful, and comprehensive.
2. Data practices must protect civil rights, prevent unlawful discrimination, and advance equal opportunity.
3. Governments at all levels, including the states, should play a role in protecting and enforcing privacy rights.
4. Legislation should provide redress for privacy violations.

Question 4: *What could be done through legislation, regulation, or by implementing best practices by credit bureaus to protect consumer data and to make sure that information contained in a credit file is accurate?*

a. With respect to **data security** for the nationwide CRAs (credit bureaus), we recommended:

i. Clear supervision authority over data security at the nationwide CRAs.
The major federal law governing data security for the credit reporting agencies – the Gramm Leach Bliley Act (GLBA) - specifically excludes the Consumer Financial Protection Bureau (CFPB) from jurisdiction over its data security provisions. See 15 U.S.C. §§ 6801(b), 6805(b)(1). While the CFPB could potentially supervise for data security under other authority, such as the prohibition against unfair, abusive or deceptive practices under Section 1031 of the Consumer Financial Protection Act, Congress should give the CFPB a clear data security mandate under both GLBA and the FCRA. The CFPB already supervises the nationwide CRAs, and it would be efficient to include data security issues in that supervision. Alternatively, Congress could provide the Federal Trade Commission (FTC) with supervision authority under GLBA. Currently, the FTC

cannot investigate proactively what is going on inside the nationwide CRAs with respect to data security, but can only react after the fact by taking enforcement action.

ii. Impose significant and hefty penalties when data breaches occur at the nationwide CRAs.

In the 115th Congress, we supported S.2289, the Data Breach Prevention and Compensation Act of 2018, introduced by Senators Warren and Warner, which gave the FTC supervision authority over data security at the nationwide CRAs and larger CRAs and also gave the FTC authority to levy significant and hefty penalties if a data breach occurred at these CRAs.

b. With respect to **accuracy of information** at the nationwide CRAs, consumer advocates recently submitted testimony to the House Financial Services Committee[1] that recommended the following reform measures:

i. Right of appeal. Congress should establish a right for consumers to appeal when they disagree about the results of a dispute. The appeal could either be to an independent unit in the credit bureau or to a regulator, such as the CFPB or FTC. If the unit is housed within a credit bureau, the unit must have direct and unfettered authority to make independent decisions and not be subject to any restrictions or incentives to process disputes quickly or in favor of furnishers.

ii. Stricter matching criteria. Congress should require the credit bureaus to use stricter matching criteria, including matching information based on all nine digits of the consumer's SSN or eight digits plus full name and address. At a minimum, the CFPB should be required to engage in a rulemaking to impose stricter requirements and to establish minimum procedures to ensure "maximum possible accuracy."

iii. Sufficient resources and independent review. Congress should clarify that the credit bureaus must devote sufficient resources and conduct independent analyses in disputes.

iv. Injunctive relief for consumers. Congress should give consumers the right to seek injunctive relief compelling credit bureaus to fix a credit report.

v. Provide a public alternative for credit reporting. Congress should establish a publicly owned alternative for credit reporting. While public agencies are far from perfect, at least they would be responsive to public pressure and government oversight. If commercial credit bureaus are not responsive to a consumer's dispute, the consumer would have the option of having a lender or other user rely on the publicly owned credit bureau.

In the 115th Congress, we supported S.1786, the Stop Errors in Credit Use and Reporting (SECURE) Act of 2017, introduced by Senator Schatz. S.1786 included almost all of these

[1] "Who's Keeping Score? Holding Credit Bureaus Accountable and Repairing a Broken System," Hearing before the H. Comm. on Fin. Serv., 116th Cong., (2019)(testimony of Chi Chi Wu, National Consumer Law Center).

reforms. On the House side, we support H.R. 3755, the Comprehensive Consumer Credit Reporting Reform Act, introduced by House Financial Services Chair Waters, which also included almost all these reforms. We have also supported the discussion draft of the CCCRA that Congresswoman Waters recently issued.

Question 5: *What could be done through legislation, regulation, or by implementing best practices so a consumer can easily identify and exercise control of data that is being (a) collected and shared by data brokers and other firms and (b) used as a factor in establishing a consumer's eligibility for credit, insurance, employment, or other purposes.*

a. **Data brokers that sell information used for credit, insurance, employment and other FCRA-covered purposes are already consumer reporting agencies and should be brought into compliance.** If a data broker is collecting and sharing data used or expected to be used as a factor in determining eligibility for credit, insurance, employment or other purpose authorized under the FCRA, that broker is a "consumer reporting agency" subject to the FCRA – period. The scope of what constitutes a "consumer report" and "consumer reporting agency" under the FCRA is not limited to Equifax, Experian and TransUnion but is quite expansive. A "consumer report" includes:

> any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for [credit, insurance, employment or other FCRA-authorized purpose].
>
> 15 U.S.C. § 1681a(d).

As one can see, this definition is not limited to credit-based information and includes very broad categories of "character, general reputation, personal characteristics, or mode of living." This encompasses almost all information about a consumer, so long as it is used for a purpose authorized by the FCRA. These permissible purposes include use for credit, employment, insurance, government benefits, licenses, and the FCRA "catch-all" purpose of a "legitimate business need for the information – (i) in connection with a business transaction that is initiated by the consumer,…" 15 U.S.C. § 1681b(a).

In turn, the term "consumer reporting agency" means:

> any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties.
>
> 15 U.S.C. § 1681a(f).

Thus, if a data broker collects and shares third-party information that constitutes a "consumer report," the data broker is a "consumer reporting agency" under the FCRA and must comply with the Act.

Unfortunately, several circuit courts have shown a reluctance to respect the plain language of the FCRA and its broad coverage. *See, e.g.,* Zabriskie v. Fed. Nat'l Mortg. Ass'n, 912 F.3d 1192 (9th Cir. 2019) (in a 2-1 decision, holding that Fannie Mae's Desktop Underwriter program is not a CRA because its role is limited to providing software that allows lenders to assemble or evaluate information; majority ignored fact that it is DU itself which actually obtains information from various sources including nationwide CRAs and that DU itself issues a recommendation); Fuges v. Southwest Title, 707 F.3d 241 (3d Cir. 2012) (objectively reasonable for company that prepared reports on current owners of properties to interpret the reports as outside the FCRA because they allegedly pertained to the property and not to the consumer -- despite the fact the reports included information on judgments personally against the consumer). These cases have undermined the FCRA and prompted certain types of specialty CRAs, such as criminal background check and tenant screening agencies, to claim they are not covered by the Act because they merely provide software to end users.

Thus, we urge Congress to require that the CFPB issue a rule or guidance clarifying that the broad scope of the FCRA already covers entities such as Southwest Title, criminal background and tenant screening agencies, and automated underwriting systems. Any rule should emphasize the existence of the catch-all permissible purpose in defining the scope of the definition. Also, the rule should clarify that a consumer report also includes reports that purport to provide information about an entity other than a consumer, e.g., a property or household or IP address, which are actually a pretext to dodge coverage because the data broker is in reality providing information about a consumer or group of consumers.

b. **A data broker bill should strengthen, not undermine, the FCRA.** One of the biggest perils of a data broker bill is the possibility it could weaken the FCRA. Some of the previously introduced data broker bills, such as S. 2025 in the 113th Congress (Sen. Rockefeller), would have significantly overlapped in coverage with the FCRA. Many of the data brokers covered by the bill would also be covered by the FCRA, which as discussed above, has a very broad definition for what constitutes a "consumer report" and a "consumer reporting agency." While these bills did include some protections similar to the FCRA, there were critical differences – the most important is that the FCRA is privately enforceable by injured consumers while the protections of this bill were not. Thus, a company that sells consumer information for FCRA-covered purposes would have a tremendous incentive to argue that it is not a consumer reporting agency under the FCRA because instead it would be covered by the provisions of the data broker law. Such an argument could find ready favor with the courts which, as discussed above, have shown a reluctance to respect the plain language of the FCRA and its broad coverage. The end result would be that fewer companies would be subject to the protections of the FCRA, to the detriment of consumers and consumer rights.

Instead of enacting a separate data broker bill, we urge Congress to expand the definition of "consumer report" and "consumer reporting agency" under the FCRA to cover data brokers who

are not already governing by the FCRA. Congress should regulate under the FCRA the following uses of personally identifiable data collected and sold by a third party:

- Marketing, including determination of which consumers receive what advertisements by postal mail or over the Internet
- Pricing of goods and services
- Fraud risk or identity verification for currently non-covered uses (*i.e.*, uses other than credit, employment, insurance, etc. which are already covered)
- College admissions

Note, however, that we do not want such uses to be permissible purposes under the FCRA to obtain credit-based consumer reports or other financial data. Thus such uses should only be permitted to obtain non-credit or non-financial data.

b. **Create a registry of all consumer reporting agencies under the FCRA, including data brokers under an expanded definition.** A registry of consumer reporting agencies, as discussed in our answer to Question 2, would help consumers identify and exercise control of data that is being collected and shared by data brokers and other firms covered by the FCRA.

* * *

Thank you for issuing the Call for Feedback on Data Privacy, Protection, and Collection. We appreciate your interest and willingness to consider reforms on this issue. If you have any questions about this response, please contact Chi Chi Wu at 617-542-8010 or cwu@nclc.org.

Respectfully submitted,

National Consumer Law Center (on behalf of its low-income clients)
Allied Progress
Americans for Financial Reform
Center for Digital Democracy
Community Service Society of New York
Consumer Action
Consumer Federation of America
Demos
East Bay Community Law Center
Jacksonville Area Legal Aid
National Association of Consumer Advocates
National Fair Housing Alliance
Privacy Rights Clearinghouse
Public Citizen
Public Justice Center
Public Law Center
The Consumer Assistance Council, Inc.
Woodstock Institute

Public Interest Privacy Legislation Principles

Unregulated data collection and use in the United States has eroded public trust in companies to safeguard and use data responsibly. Surveys show that, while individuals often try to remove or mask their digital footprints,[1] people think they lack control over their data,[2] want government to do more to protect them,[3] and distrust social media platforms.[4]

The current U.S. data privacy regime, premised largely upon voluntary industry self-regulation, is a failure. Irresponsible data practices lead to a broad range of harms, including discrimination in employment, health care, and advertising, data breaches, and loss of individuals' control over personal information. Existing enforcement mechanisms fail to hold data processors accountable and provide little-to-no relief for privacy violations.

The public needs and deserves strong and comprehensive federal legislation to protect their privacy and afford meaningful redress. Privacy legislation is essential to ensure basic fairness, prevent discrimination, advance equal opportunity, protect free expression, and facilitate trust between the public and companies that collect their personal data. Legislation should reflect at least the following ideas and principles:

1. Privacy protections must be strong, meaningful, and comprehensive

Privacy concerns cannot be fully addressed by protecting only certain classes of personal data held by some companies. Legislation should mandate fairness in all personal data processing, respect individuals' expectations for how data should be treated, provide for data portability, and include safeguards against misuse of data, including de-identified and aggregate data. Legislation should advance fundamental privacy rights and require all entities that collect, store, use, generate, share, or sell (collectively, "process") data both online and offline to comply with Fair Information Practices[5] (collection limitation, data

---

[1] *The State of Privacy in Post-Snowden America*, Pew (Sept. 21, 2016), http://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america.
[2] Bree Fowler, *Americans Want More Say in the Privacy of Personal Data*, Consumer Reports (May 18, 2017), https://www.consumerreports.org/privacy/americans-want-more-say-in-privacy-of-personal-data.
[3] Lee Rainie, *Americans' Complicated Feelings About Social Media in an Era of Privacy Concerns*, Pew (Mar. 27, 2018), http://www.pewresearch.org/fact-tank/2018/03/27/americans-complicated-feelings-about-social-media-in-an-era-of-privacy-concerns.
[4] *Id.*
[5] Fair Information Practices are similar to those adopted by the OECD. *See* OECD Privacy Framework, http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

quality, purpose specification, use limitation, security safeguards, openness, access and correction rights, and accountability) across the complete life cycle of the data. Legislation should require all data processing to be clearly and accurately explained, justified, and authorized by the individual. People should have the right to know when their data has been compromised or otherwise breached. Additionally, legislation should require entities processing data to adopt technical and organizational measures to meet these obligations, including risk assessments of high-risk data processing.

2. Data practices must protect civil rights, prevent unlawful discrimination, and advance equal opportunity

Legislation should ensure fundamental fairness of and transparency regarding automated decision-making. Automated decision-making, including in areas such as housing, employment, health, education, and lending, must be judged by its possible and actual impact on real people, must operate fairly for all communities, and must protect the interests of the disadvantaged and classes protected under anti-discrimination laws. Legislation must ensure that regulators are empowered to prevent or stop harmful action, require appropriate algorithmic accountability, and create avenues for individuals to access information necessary to prove claims of discrimination. Legislation must further prevent processing of data to discriminate unfairly against marginalized populations (including women, people of color, the formerly incarcerated, immigrants, religious minorities, the LGBTQIA/+ communities, the elderly, people with disabilities, low-income individuals, and young people) or to target marginalized populations for such activities as manipulative or predatory marketing practices. Anti-discrimination provisions, however, must allow actors to further equal opportunity in housing, education, and employment by targeting underrepresented populations where consistent with civil rights laws. Moreover, decades of civil rights law have promoted equal opportunity in brick-and-mortar commerce; legislation must protect equal opportunity in online commerce as well.

3. Governments at all levels should play a role in protecting and enforcing privacy rights

The public consistently call for government to do more, not less, to protect them from misuse of their data. Legislation should reflect that expectation by providing for robust agency oversight, including enhanced rulemaking authority, commensurate staff and resources, and improved enforcement tools. Moreover, no single agency should be expected to police all data processors; therefore, legislation should empower state attorneys general and private citizens to pursue legal remedies, should prohibit forced arbitration, and importantly, should not preempt states or localities from passing laws that establish stronger protections that do not disadvantage marginalized communities.

4. Legislation should provide redress for privacy violations

Individuals are harmed when their private data is used or shared in unknown, unexpected, and impermissible ways. Privacy violations can lead to clear and provable financial injury, but even when they do not, they may, for example, cause emotional or reputational harm; limit awareness of and access to opportunities; increase the risk of suffering future harms; exacerbate informational disparities and lead to unfair price discrimination; or contribute to the erosion of trust and freedom of expression in society. In recognition of the many ways in which privacy violations are and can be harmful, legislation should avoid requiring a showing of a monetary loss or other tangible harm and should make clear that the invasion of privacy itself is a concrete and individualized injury. Further, it should require companies to notify users in a timely fashion of data breaches and should make whole people whose data is compromised or breached.

Signed,

Access Humboldt
Access Now
Berkeley Media Studies Group
Campaign for a Commercial-Free Childhood
Center for Democracy & Technology
Center for Digital Democracy
Center for Media Justice
Center on Privacy & Technology at Georgetown Law
Color of Change
Common Cause
Common Sense Kids Action
Consumer Action
Consumer Federation of America
Consumers Union
Customer Commons
Demand Progress
Free Press Action Fund
Human Rights Watch
Lawyers' Committee for Civil Rights Under Law
Media Alliance
Media Mobilizing Project
National Association of Consumer Advocates
National Consumer Law Center
National Consumers League
National Digital Inclusion Alliance
National Hispanic Media Coalition
New America's Open Technology Institute
Oakland Privacy
Open MIC (Open Media and Information Companies Initiative)
Privacy Rights Clearinghouse
Public Citizen
Public Knowledge
U.S. PIRG
United Church of Christ, OC Inc.